

Persistent Behaviour Tracing (PBT)



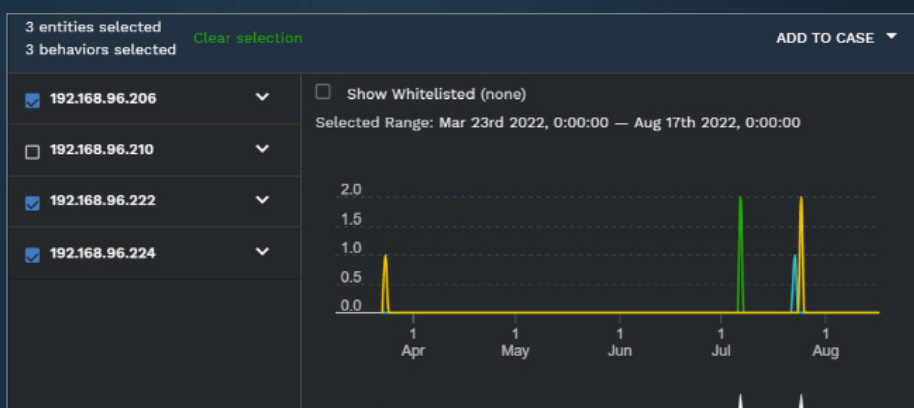
Cyber threats increasingly exploit gaps in an organization's security posture created by isolated data pools of security products and the challenges associated with query-based analysis. Query-based analysis requires large amounts of data to be online or restored from backups to search.

SilverSky has a unique method of storing reduplicated behaviour attributes associated with each event on a per entity basis. This allows for a historical contextual view over an unlimited time-frame without massive storage requirements. We call it Persistent Behaviour Tracing (PBT).

Find Threats Others Miss, Fill Gaps In Your Security Posture

PBT utilizes a unique hash sum, calculated at processing time, from fields describing each behaviour. PBT identifies behaviours via a variety of detection methods determined by the analytics that generate that behaviour and each occurrence of a behaviour is then tracked using a set of fields specific to that behaviour. The result is a system that tracks attack vectors in real-time, saves relations indefinitely, and identifies associations based on the threat behaviour.

Persistent Behaviour Tracing (PBT) Example Web Server Attack, Multiple Source IPs



197
days

average time
to detect a breach

Identify correlations
between threat signals
over all time

Eliminate extensive and
expensive log management
hot storage requirements

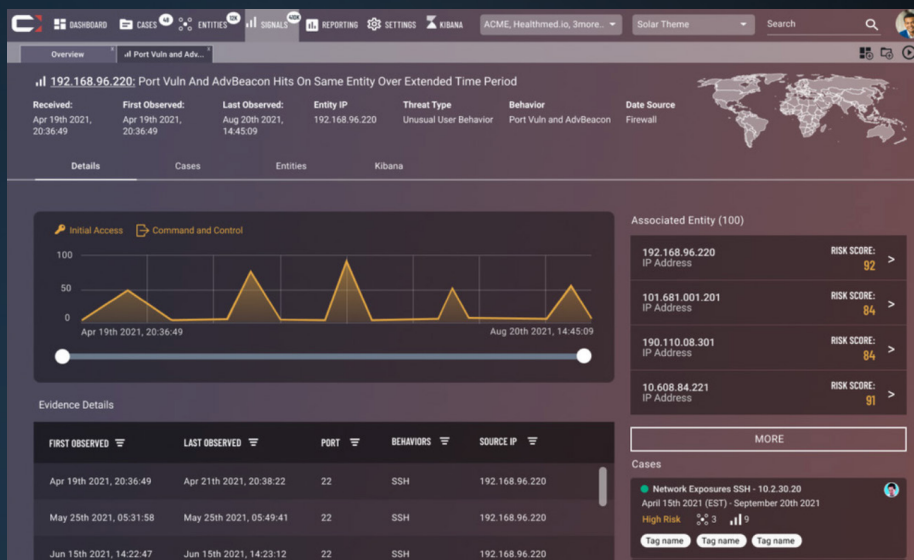
Streaming analytics
identify threats in real-time
vs. batch processing

Dramatically increase
security analyst accuracy
and efficiency

Increase Analyst Efficiency and Reduce Storage Costs

Analysts spend an extraordinary amount of time investigating suspicious activity. Traditional SIEM and even SOAR products treat alerts and events in isolation and utilize batch processing. PBT eliminates the need for manual queries and accelerates resolution with historical contextual views with all the relevant attributes in a single dashboard.

Organizations often have to weigh the benefit of maintaining vast amounts of log data in hot storage versus the incurred cost of that storage. PBT's unique hash sum deduplication eliminates the need for massive volumes of expensive hot storage. PBT also eliminates the need for backup-restores and the delays and complexity associated with them. This opens up the window for investigation and research since there are no disruptive, complex and time-prohibitive delays that prevent analysts from fully researching potential threats.



“

Leveraging Artificial Intelligence and Machine Learning is the only way to have a shot at analysing the mountains of data coming from so many different systems.

Analysing and correlating event logs with the necessary intelligence is long overdue in the security space and SilverSky delivers.

- International Media Company

”

Call SilverSky 1-800-234-2175

 [linkedin.com/company/silversky](https://www.linkedin.com/company/silversky)

 twitter.com/silversky

www.silversky.com



1-800-234-2175

learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560